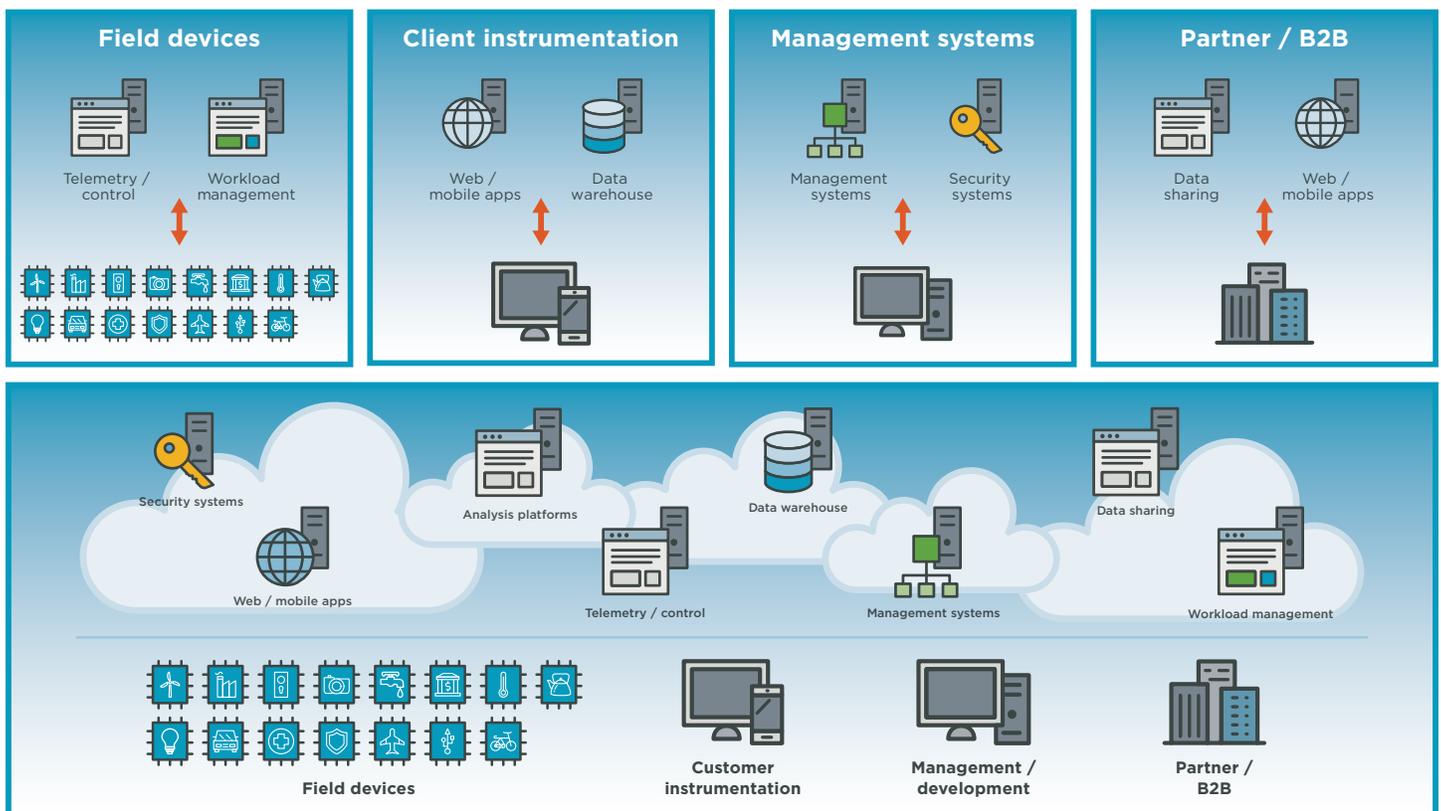# Internet of Things device security

Test your IoT solution from field devices to the cloud.

The number of connected devices has skyrocketed in the past few years thanks to modern technology. Because of IoT's rapid evolution, innovative disruptions are occurring at a staggering pace. From Bluetooth speakers to toothbrushes, connected devices have become a significant target for exploitation by threat actors.

To test all of the components of an IoT device that may be exposed to threats, you need an end-to-end testing strategy. Coalfire's unique approach to IoT penetration testing addresses this ecosystem completely and covers communication technologies, cloud-based data management platforms, data-sharing application programming interfaces (APIs), and management and instrumentation web and mobile apps.

Field devices

Telemetry / control Workload management

Client instrumentation

Web / mobile apps Data warehouse

Management systems

Management systems Security systems

Partner / B2B

Data sharing Web / mobile apps

Security systems

Web / mobile apps

Analysis platforms

Telemetry / control

Data warehouse

Management systems

Data sharing

Workload management

Field devices

Customer instrumentation

**Management / development**

Partner / B2B

Our extensive experience testing a variety of internet-connected devices spans automotive environments, security systems, building automation, and IoT solution integrators. We have a lab that contains state-of-the-art equipment that can execute a wide variety of attack vectors across almost any type of hardware. Our testing capabilities include:

- Joint Test Action Group (JTAG), universal asynchronous receiver-transmitter (UART), controller area network (CAN), and serial peripheral interface (SPI)

- Basic input/output system (BIOS), general-purpose input/output (GPIO), inter-integrated circuit (I2C), and more

- Side channel attacks

- Electrically erasable programmable read-only memory (EEPROM) reader/writer

- Radio frequency (RF) capabilities

- Physical bypass

- Reverse engineering

- Custom control assemblies

WHY PARTNER WITH COALFIRE FOR IOT PENETRATION TESTING?

- We've completed hundreds of projects in industrial environments, dozens of projects for the automotive industry, and numerous projects for medical device manufacturers.

- We have more than 70 teams of testers who work on all of the largest cloud service providers' IoT service platforms. These testers possess a deep understanding of the platforms that optimize the rapid deployment of IoT solutions.

- Coalfire Labs R&D has top-class testing capabilities, including a dedicated hardware lab that contains state-of-the-art equipment that enables us to perform testing on a wide range of devices.

- We continuously monitor the evolving threat landscape and help further the industry through speaking engagements, tools, process development, and publications.

- We bring a deep understanding of the risks associated with legacy and cutting-edge technologies and how they impact government and commercial organizations. This understanding allows our team to detect vulnerabilities across a wide range of technologies, especially new and emerging ones.

DS_IoT_012820
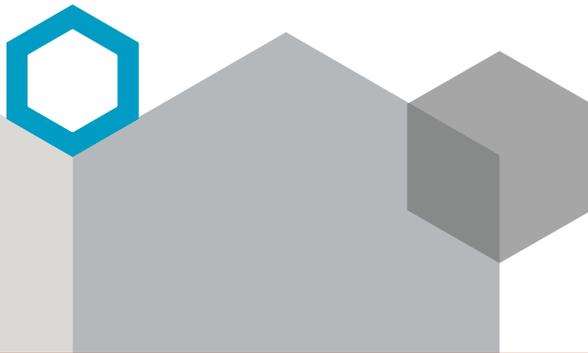
PROTECT EVERY ASPECT OF YOUR IOT DEVICE WITH A COMPREHENSIVE TESTING APPROACH.

Learn more about Coalfire's IoT device security services.

Coalfire.com | 877.224.8077

COALFIRE.

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com**